ABSTRACT OF THE DISCLOSURE

A digital certificate management apparatus updates a proof key used for proving validity of a digital certificate used for authentication for establishing communication between a client and a server. The apparatus acquires a new proof key for updating, acquires a new digital certificate used for the authentication for which validity can be proved with the use of said new proof key, transmits the new proof key to the client and transmits a new server certificate which is a new digital certificate for the server to the server. The apparatus transmits the new server certificate to the server after receiving, from the client, information indicating that the client has received the new proof key.